基于双线性配对的 Ad hoc 网络混合门限签名方案*

黄素珊, 钱海峰
(华东师范大学 计算机科学与技术系, 上海 200062)

摘 要: 为了解决 Ad hoc 网络中的签名及密钥安全问题,利用双线性配对的优点,结合混合门限签名机制,设计了适用于 Ad hoc 网络的基于双线性配对的混合门限签名算法。该算法可以有效提高网络传输效率、节省数据传输量,在安全性及效率上更能满足 Ad hoc 网络及传感器网络的需要。

关键词: Ad hoc 网络; 双线性配对; 门限签名; 门限共享秘密; 网络安全; 传感器网络
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)08-3064-03
doi:10.3969/j.issn.1001-3695.2010.08.67

Bilinear-pairing based hybrid threshold signature scheme in Ad hoc network

HUANG Su-shan, QIAN Hai-feng
(*Dept. of Computer Science & Technology, East China Normal University, Shanghai* 200062, *China*)

Abstract: In order to improve the signature and secret key security in Ad hoc network, this paper proposed a bilinear-pairing based hybrid threshold signature scheme which was based on bilinear-pairing and combined with hybrid threshold signature. The proposed scheme can not only improve the network transmission efficiency and save bandwidth, but also make the security and efficiency more suitable for the Ad hoc and sensor network.

Key words: Ad hoc network; bilinear pairing; threshold signature; threshold shared secret; network security; sensor network

Ad hoc 网络是一种新型网络结构,网络中的节点由装配着无线收发装置的移动终端构成,并通过传输范围有限的移动终端间的互相协作和自我组织来实现网络的互连以及数据传输,它的出现推动了在任意环境下自由通信技术的发展进程。由于这种网络具有无中心、自组织、动态拓扑等特点,目前在军事、民用和商业领域中都有着广泛的应用。但是由于无线通信的信号容易获取,Ad hoc 网络很容易造成信息泄漏。因此,需要采用有效的措施来保证路由信息和数据的私密性。同时自组织的节点容易受到攻击,被攻破并俘获的概率较大,因此需要加强对每个节点中自身密钥的保护以加强 Ad hoc 网络的安全。另一方面,Ad hoc 中的节点主要由无线传感器组成,网络资源有限,从而使得需要大量数据交互的传统签名不再适用。

对于密钥容易被泄露的问题,在 1991 年,Desmedt 等人[1]率先提出了基于 RSA 的(t,n)门限数字签名方案,随后基于不同公钥密码体制的门限签名方案被陆续提出[2]。在(t,n)门限签名中,通常把密钥拆分成 n 份,分别由 n 个成员持有。只有 t 个或者 t 个以上的成员才能生成合法签名,从而减少了单个成员密钥泄露造成的危险。这对节点容易被入侵的 Ad hoc 网络来说,非常具有吸引力。Ad hoc 网络中的每个节点可以把密钥拆分后由 n 个周围节点共享,通过门限签名来保护密钥。但是,(t,n)门限签名的密钥共享技术大多采用多项式插值原理,当群体内部的恶意成员数大于门限值 t 时,他们合作就有可能获取密钥,进而假冒节点签名[3]。文献[4]提出了抵抗成员欺骗的方法,但是计算量较大。文献[5]提出了一种应用于服务器协助的混合门限签名,解决了参与门限签名成员不完全可信的情况下,通过赋予不同成员签名的权重,从而防止恶意成员合谋伪造签名。但是,文章只给出了一个框架思路,没有具体的实现。

针对以上几个问题,本文在现有密码体制的基础上提出了适用于 Ad hoc 网络的基于双线性配对的门限签名算法。该方案利用双线性配对从而减少了密钥长度,提高运算速度,以适应 Ad hoc 网络对带宽要求高的特点。同时根据文献[5]的思路,在基于双曲线配对的门限签名方案中加入混合签名机制,即把签名的成员分为两类:一个签名者和 n 个参与者,只有签名者主动要求签名后,同时在 n 个参与者中有 t 个参与者参与签名,才能生成合法的签名,从而防止了在群密钥共享中,t 个或者多于 t 个成员就可以冒充签名者的情况。

1 相关概念

1.1 双线性映射

设 G_1, G_2 分别是同为 q 阶的加群和乘群,并且假设 P 为 G_1 的生成元。假设在群 G_1, G_2 中,离散对数问题是难解的。可以定义双线性映射对为 $e:(G_1 \times G_1 \to G_2)$ 并且满足以下特性:

a)双映射性。$e(aP,bP') = e(P,P')^{ab}$,对所有的 $P, P' \in G_1$,所有的 $a, b \in \mathbb{Z}_q^*$ 成立。

b)非退化性(non-degenerate)。如果 $e(P,P') = 1$,存在 $P' \in G_1$,则有 $P = 0$。

c) 可计算性。存在有效的算法,对于 $P, P' \in G_1$,可计算 $e(P,P')$。

收稿日期: 2009-09-27; **修回日期**: 2010-03-12 **基金项目**: 国家自然科学基金资助项目(60703004, 60873217, 60703031);国家教育部博士点基金资助项目(20070269005)

作者简介:黄素珊(1984-),女(壮族),广西柳州人,硕士,主要研究方向为信息安全、密码学等(snowsnowhss@163.com);钱海峰(1977-),男,副教授,博士,主要研究方向为信息安全、密码学.

当在群中,CDHP(computational Diffie Hellman)问题难解而 DDHP(decision Diffie Hellman problem)易解时,称该群为 GDH 群(gap Diffie Hellman group)。双线性映射可以由 Weil 映射和 Tate 映射得到。

1.2　混合门限签名

混合门限签名是把只有两个参与者的门限签名和具有多个参与者的门限签名结合起来的签名方案。方案由以下三个部分组成:

a)初始化。假定(X,Y)为签名者 S 用于生成签名的公私钥对,有 n 个签名的参与者 $P_i(i=1,\cdots,n)$,要生成合法的签名至少需要 t 个或者 t 个以上的参与者。首先,签名者 S 拆分私钥 $X \xrightarrow{(2,2)} (X_s,X_p)$,$X_s$ 由签名者 S 持有。接着,签名者 S 通过合适的密钥共享方案拆分 $X_p \xrightarrow{(t,n)} (X_p^{-1},\cdots,X_p^n)$,每个参与者 P_i 持有部分私钥 X_p^i。

b)签名。首先,签名者 S 生成部分签名 $\sigma_s=g(m,X_s)$,g 为签名算法。接着,参与者 P_{i_j} 生成自己的部分签名 $\sigma_p^{i_j}=g_1(m,X_p^{i_j})$。其中,$g_1$ 为签名生成算法,$1\leqslant i_j\leqslant n$,$1\leqslant j\leqslant w$,$t\leqslant w\leqslant n$。任何人只要持有多于 w 个参与者的有效签名就能计算出 $\sigma_p=g_2(\sigma_p^{i1},\cdots,\sigma_p^{iw})$。其中,$g_2$ 相应的签名合成算法,$1\leqslant i_j\leqslant n$,$1\leqslant j\leqslant w$,$t\leqslant w\leqslant n$。$\sigma_s$,$\sigma_p$ 生成后,持有这两个部分签名的人,可以得到最终的合法的签名 $\sigma=g_2'(\sigma_s,\sigma p)$,其中,$g_2'$为相应的签名合成算法。

c)验证。验证算法根据签名 σ、公钥 Y 和消息 m 验证 σ 是否合法,如果合法则返回真,否则返回假。

定理 1　如果混合门限签名是不可伪造的且强壮的,则此混合门限签名是安全的。

证明　参见文献[6]。

2　基于双线性配对的混合门限签名设计

由于 Ad hoc 网络自身的特点,传统的方法不能直接使用。根据文献[7]提出的安全要求,本文提出了在 Ad hoc 网络中密钥管理及签名方案应满足以下几点要求:

a)允许节点动态变化,包括新节点的加入和原有节点的退出;

b)采用的门限签名方案如何抵抗合谋攻击;

c)Ad hoc 网络中的节点在能源、带宽、计算能力、存储能力等方面均有限制。故而应用于 Ad hoc 网络中的算法必须考虑节点能源的合理利用,如何实现方案的安全性与计算量的平衡。

其中,要求 a)b)在文章的安全性分析章节给出具体的分析。要求 c)在算法的各个部分都要考虑,具体的性能指标比较在第 4 章中给出。

签名方案流程描述如下:假设 Ad hoc 网络由 n 个节点组成,其中,需要生成签名的成员为签名者 S,参与签名的成员为参与者 P_i。首先,在初始化时,签名者 S 选择自己的主密钥 s 并广播相关的系统参数。随后,签名者 S 把主密钥拆分为两部分,一部分签名者由持有,另一部分通过(t,n)门限方案被所有节点共享,同时主密钥从 S 保存的信息中删除。在签名阶段,签名者对消息生成部分签名后,把需要签名的消息和相关参数发送给参与者 P_i,当获得 t 个或者 t 个以上合法的签名片段后,就可以恢复出完整的签名。

具体方案分为四个阶段,即方案初始化阶段、数据交换阶段、门限签名生成阶段和签名验证阶段。

2.1　方案初始化

令 G_1 为由 P 生成的 q 阶循环加法群,G_2 为具有相同阶 q 的循环乘法群。双线性配对映射:$e:(G_1\times G_1)\to G_2$。定义哈希函数 $H_1:\{0,1\}^*\to G_1$。签名者 S 首先选择一个随机数 $s\in\mathbb{Z}_q^*$,s为这个方案的主密钥,然后计算 $P_{\text{pub}}=sP$ 并公布系统参数为 $G_1,G_2,q,e,P,P_{\text{pub}},H_1$。

2.2　数据交换

假定有一个签名者 S 和 n 个参与者 $P_i(i=1,\cdots,n)$。签名者 S 选择一个随机数 $s_1\in\mathbb{Z}_q^*$ 作为签名者的部分私钥,计算 $s_2=s-s_1$作为另一部分私钥,然后,S 随机选择一个$(t-1)$次的多项式,即$f(x)=a_{t-1}x^{t-1}+\cdots+a_1x+s_2$。其中:$a_j\in_R\mathbb{Z}_q^*(j=1,\cdots,t-1)$。

每个参与者 P_i 的部分私钥为 $x_i=f(i)$,$i=1,\cdots,n$,由签名者通过安全信道发送给每个参与者 P_i。此时,签名者删除 s,s_2 只保留自己的部分私钥 s_1。

2.3　门限签名生成

$m\in\{0,1\}^*$为签名者 S 需要签名的信息。签名步骤如下:

a)签名者。生成的部分签名为 $\sigma_1=s_1H_1(m)$,同时把 m 发送给参与者 $P_i(i=1,\cdots,n)$。

b)参与者。每个参与者 P_i 分别计算自己的部分签名 $\sigma_2^i=x_iH_1(m)$。当签名者收到 t 个或 t 个以上的部分签名 σ_2^i 后,就可以计算出:

$$\sigma_2=\sum_{i=1}^{t}\lambda_i\sigma_i=\sum_{i=1}^{t}\lambda_i f(i)H_1(m)=f(0)H_1(m)=s_2H_1(m)$$

其中:$\lambda_i=\dfrac{\prod_{j=1,j\neq i}^{t}(0-j)}{\prod_{j=1,j\neq i}^{t}(i-j)}\bmod q$。

c)当签名者获得两部分签名后,可以得到最终的签名 $\sigma=\sigma_1+\sigma_2$。

2.4　签名验证

在验证消息 m 的签名(σ,P)时,只需验证等式 $e(\sigma,P)=e(H_1(m),P_{\text{pub}})$是否成立,如果成立则签名合法,否则失败。因为 $e(\sigma,P)=e(sH_1(m),P=e(H_1(m),P_{\text{pub}})$。

3　算法安全性分析

由于 Ad hoc 网络的特点,相对有线网络而言,其更易于受到攻击者的攻击。本文在以下几个方面来分析算法的安全性。

3.1　不可伪造性

方案中采取了混合门限签名的机制,对不同的签名者予以不同的权重。因此,对于不可伪造性的分析,应分为两种情况(如签名者的私钥被泄露):

a)s_1 泄密,但最多只能有 $t-1$ 个参与者泄密,即 s_2 依然是安全的。在这种情况下,即使 s_1 被攻击者获得,攻击者也只能获取部分签名 σ_1,由于仍然无法获得多于 $t-1$ 个参与者的部分签名,仍然无法伪造签名。

b)s_2 泄密,即至少有 t 个参与者的私钥泄露了,但 s_1 依然是安全的。在这种情况下,即使攻击者攻破了 t 个或者更多的参与者,只要没有签名者的参与,仍然无法伪造出合法的签名,从而防止了多个参与者合谋攻击。

由 2.2 和 2.3 节可知,成员的私钥只有节点自己知道,恶

意攻击者不知道成员的密钥就无法产生合法的部分签名,也就无法产生合法的完整签名。同时,攻击者不能从用户签名中计算成员的密钥,因为签名算法的安全性是建立在 CDH 的困难性假设基础之上,可证明随机预言模型下是安全的。

3.2 强壮性

如果 t 或者更多的成员合谋,可以获取他们自己的密钥及由此产生的部分签名,根据门限签名的构造过程式可知,完整签名由每个成员的部分签名组成,由于成员的部分私钥只有成员自己知道,他们无法获取其他成员的密钥。群中 t 或更多的成员合谋无法获取其他成员的有效密钥,从而他们无法假冒其他成员生成有效的完整签名,从而可以抵抗合谋攻击。

3.3 有效性

在本文(t,n)的门限方案中,使用了 Shamir 秘密共享机制来拆分参与者 P_i 的部分私钥 s_2,把它拆分为 n 份。因此,参与者 P_i 根据协议运行等到部分签名后,只要有 t 或者多于 t 个部分签名,就可以生成有效的参与者的部分签名,而 $t-1$ 或者少于此的参与者无法生成合法的部分签名。因此,方案是有效的(t,n)门限签名方案。

通过上面的分析讨论,本文验证了方案的正确性和安全性。

4 形式化证明

在形式化证明中,通过定理以分析此方案的安全性。

证明 1 此方案是强壮的(t,n)混合门限签名方案。

证明 此方案满足强壮性的需要。因为即使所有参与者不根据协议来执行,他们仍然不能伪造出签名。

通常来说,要知道部分私钥需要有至少 t 个参与者参与。为了不失一般性,假设 t 个参与者为 $B_1,B_2,\cdots,B_t$。其余的参与者为 $B_l,(k+1\leqslant l\leqslant n)$,$F(l)=\sum_{i=1}^{t}\lambda_i F(i)$。其中:$\lambda_i=\dfrac{\prod_{j=1,j\neq i}^{t}(l-j)}{\prod_{j=1,j\neq i}^{t}(i-j)} \bmod q$。

而且,s_2 也能由此计算出,即

$$s_2=F(0)=\sum_{i=1}^{t}\lambda_i F(i)。其中\ \lambda_i=\frac{\prod_{j=1,j\neq i}^{t}(0-j)}{\prod_{j=1,j\neq i}^{t}(i-j)} \bmod q。$$

然而,由于 CDH 问题是困难的,所以要从 P_{pub},σ 中计算出主密钥 s 也是困难的。因此,主密钥是安全的并且强壮的。

另一方面,主密钥 s 拆分成 s_1,s_2。即使有多于 t 个参与者的私钥泄露,只要没有签名者的参与,依然不能生成合法的签名。证明毕。

5 仿真实验

为了进一步评估本算法的性能,现利用 Glomosim[8] 仿真库来建立实验平台,仿真 Ad hoc 网络,并对文献[9]和本文算法进行仿真实验,并计较两者的性能。为了便于比较,现定文献[9]算法为 TRSA,本文算法为 TBS。由于两个算法同为应用于 Ad hoc 网络的门限算法,因此具有一定的可比性。两者的不同之处在于,签名算法不同,一个为 RSA 签名,一个为基于双线性配对的签名。同时,两者的门限算法也不同,一个使用普通(t,n)门限,一个使用混合门限。因此,除了比较两者密钥生成时间外,平均延时时间也是这两个算法的性能参数。仿真实验的环境为 Windows XP/Microsoft Visual Studio 2003。主要参数如表 1 所示。

表 1 仿真实验主要参数

参数	值	参数	值	参数	值
仿真节点数	20 ~ 60	时间	10 min	节点分布	随机
门限值	6	区域	300 m × 300 m		

影响 Ad hoc 网络的因素很多,例如网络负载、网络规模、节点移动等。本文的仿真主要针对在不同网络规模下,两种算法的性能比较。因为网络规模的变化,即网络中的节点数的增减是影响门限签名的最主要因素。具体采用两组数据进行比较:密钥生成时间及端到端得平均延时。

比较结果如图 1、2 所示。

图 1 表示两种算法生成密钥所需时间。可以看出,随着节点数的增加,网络规模也增大,因此所需的时间也增加。同时,由于 TBS 需要经过两次逆运算,因此耗时要稍微长些。

图 2 表示两种算法的平均延时。随着节点数的增加 TBS 比 TRSA 快。

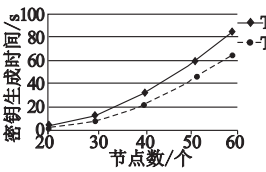

图1 密钥生成时间比较

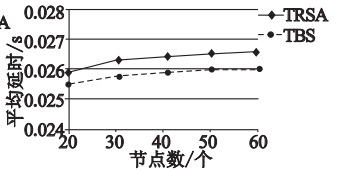

图2 平均延时时间比较

6 结束语

随着信息技术的不断发展,人们对移动通信的需求也越来越强。目前,Ad hoc 网络已经逐渐成熟和实用,对其研究已成为公开热点。但是,对 Ad hoc 网络的安全性研究还处于起步阶段,成为其实用化的一个瓶颈。本文在基于双线性配对签名的基础上,同时采用混合门限签名的机制,对不同的签名参与者进行权重划分,从而在安全性、实用性、效率性等方面更符合 Ad hoc 网络的要求。

同时,Ad hoc 网络的安全问题也是个极为复杂的开发问题。其中,例如新加入节点的可信度判定问题,被入侵节点的侦测与废除问题,周围节点低于门限值等问题都还有待研究。如何进一步完善 Ad hoc 网络的安全仍是今后研究的重点。

参考文献:

[1] DESMEDT Y, FRANKEL Y. Shared generation of authenticators and signatures[C]//Proc of Advances in Cryptology Crypto' 91. Berlin: Springer-Verlag, 1991:457-469.

[2] 王斌,李建华. 无可信中心的(t,n)门限签名方案[J]. 计算机学报, 2003, 26(11):1581-1584.

[3] XIE Qi, YU Xiu-yuan. A new (t,n) threshold signature scheme with standing the conspiracy attack [J]. Wuhan University Journal of Natural Sciences, 2005, 10(1):107-110.

[4] WANG G L, QING S H. Weaknesses of some threshold group signature schemes[J]. Journal of Software, 2005, 11(10):1326-1332.

[5] 何明星,范平志,袁丁. 一个可验证的门限多秘密共方案[J]. 电子学报, 2006, 30(4):540-543.

[6] XU S, SANDHU R. Two efficient and provably secure schemes for server-assisted threshold signature[C]// Topics in Cryptology- CT RSA. Berlin: Springer-Verlag, 2003: 355-372.

[7] 罗传军,李飞,郎昆. Ad hoc 网络路由协议安全模型研究[J]. 西华大学学报, 2009, 28(1):36-41.

[8] BAJAJ L, TAKAI M, AHUJA R, *et al*. A scalable network simulation environment[R]. Los Angeles: UCLA Computer Science Department Technical Report, 1997.

[9] GENNARO R, HALEVI S, KRAWCZYK H, *et al*. Threshold RSA for dynamic and ad hoc group[C]// Proc of Advances in Cryptology-EUROCRYPT. Istanbul:[s.n], 2008: 88-107.

[10] WANG B, LI H. (t,n) threshold signature scheme without a trusted party[J]. Journal of Computers, 2008, 26(11):1581-1584.